Lab 278

Morris & Opazo

aws re/start

Protección de datos mediante encriptación

INTRODUCCIÓN

En este laboratorio, se conectará a un servidor de archivos que está alojado en una instancia de Amazon EC2. Configurará la interfaz de línea de comando (CL) de AWS Encryption en la instancia Creará una clave de cifrado usando AWS KMS. La clave se usará para cifrar y descifrar datos. A continuación, creará múltiples archivos de texto que, de forma predeterminada, no están cifrados. Luego usará la clave de AWS KMS para cifrar los archivos y verlos mientras se cifran. Finalizará el laboratorio al descifrar los mismos archivos y ver los contenidos.

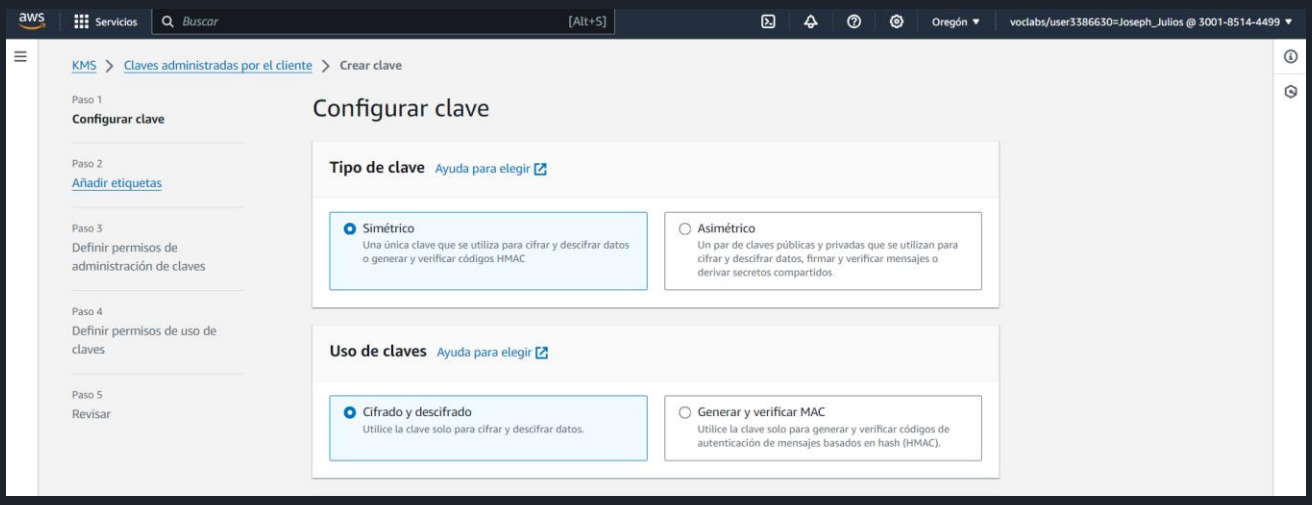
OBJETIVOS

- Configurar Crear una clave de cifrado de AWS KMS
- Instalar la CLI de AWS Encryption
- Cifrar datos de texto simple
- Descifrar texto cifrado.

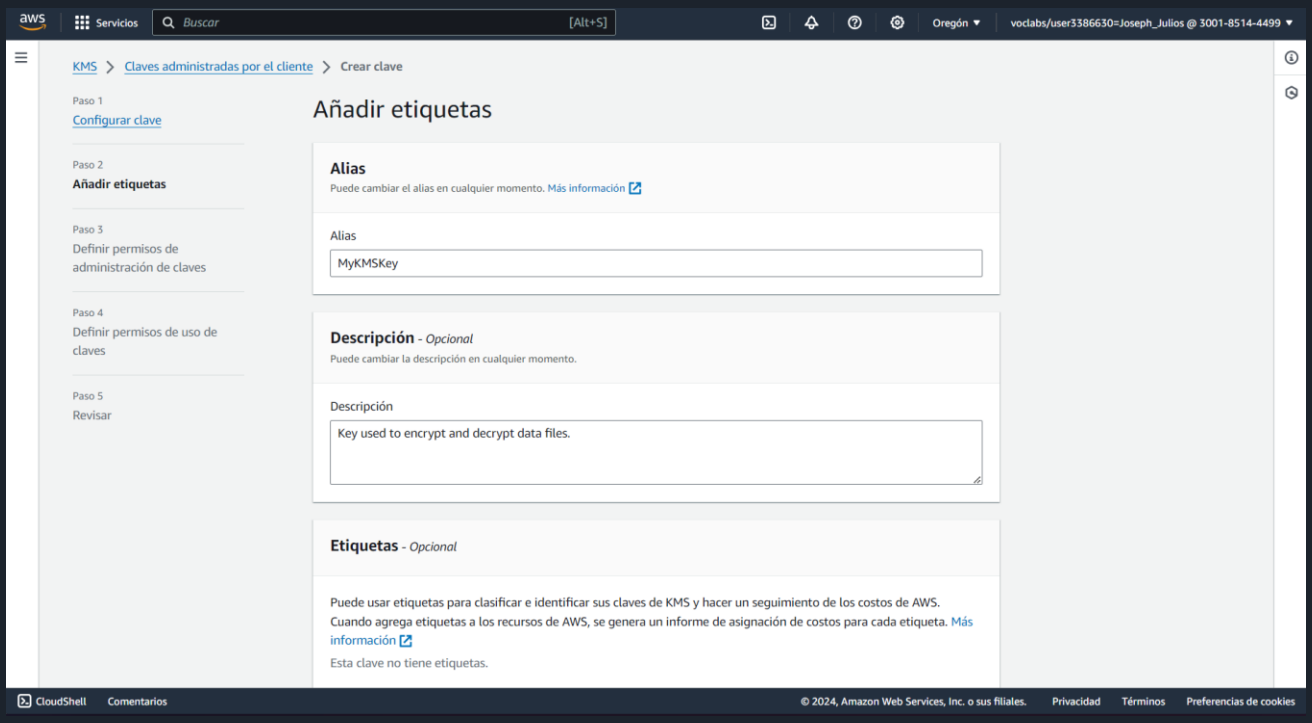
TAREA 1

Con AWS KMS, puede crear y administrar claves criptográficas y controlar su uso a lo largo de una amplia variedad de servicios de AWS y en sus aplicaciones. AWS KMS es un servicio seguro y resiliente que usa módulos de seguridad de hardware (HSM) que están validados por el Estándar de procesamiento de información federal (FIPS) Publicación 140-2, o están en el proceso de ser validados, para proteger sus claves.

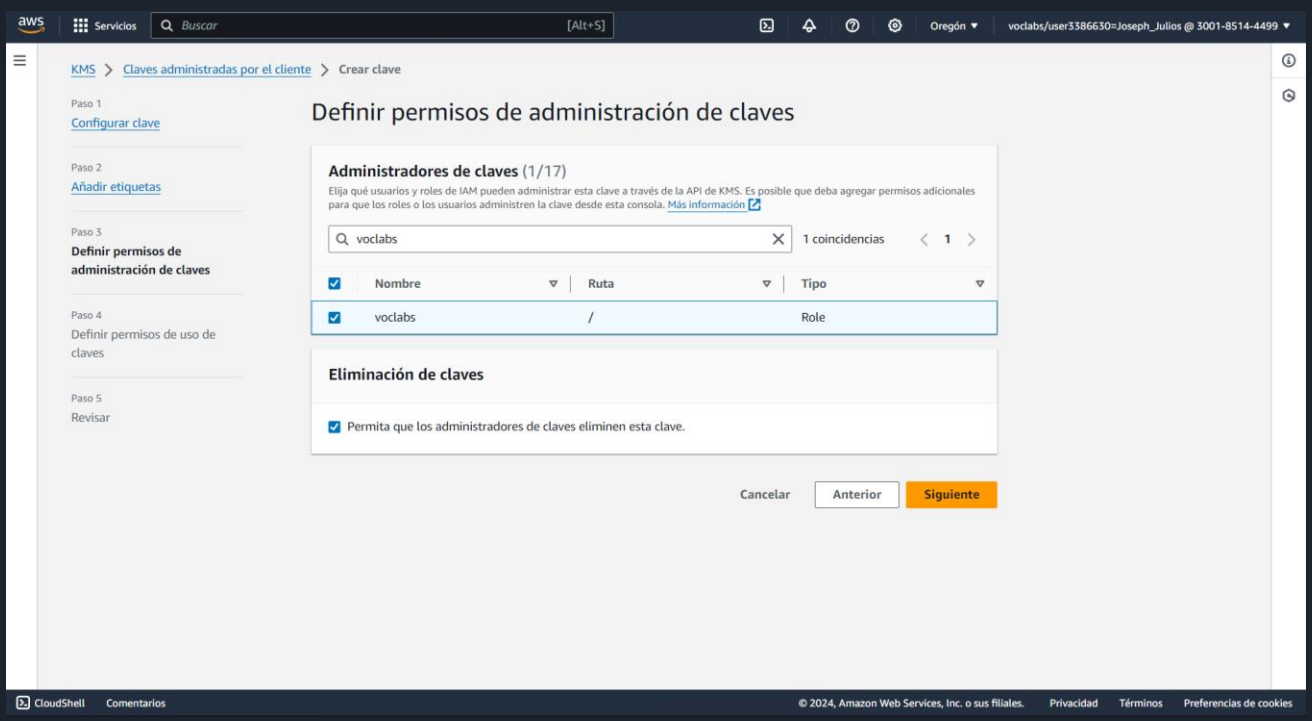
- En la consola, ingrese KMS en la barra de búsqueda y luego seleccione Key Management Service.
- Seleccione Create a key.
- En Key type, seleccione Symmetric y luego seleccione Siguiente.



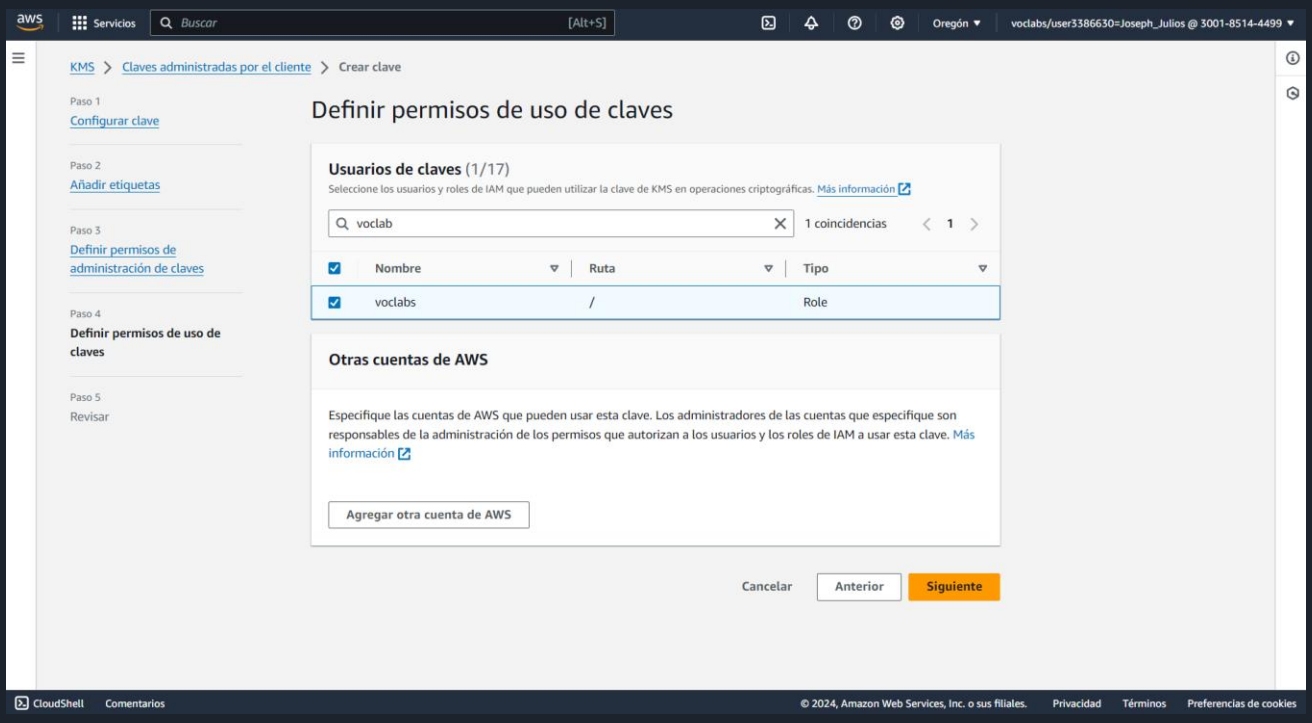
- En la página Add labels configurar Alias y descripción. Seleccione Next.



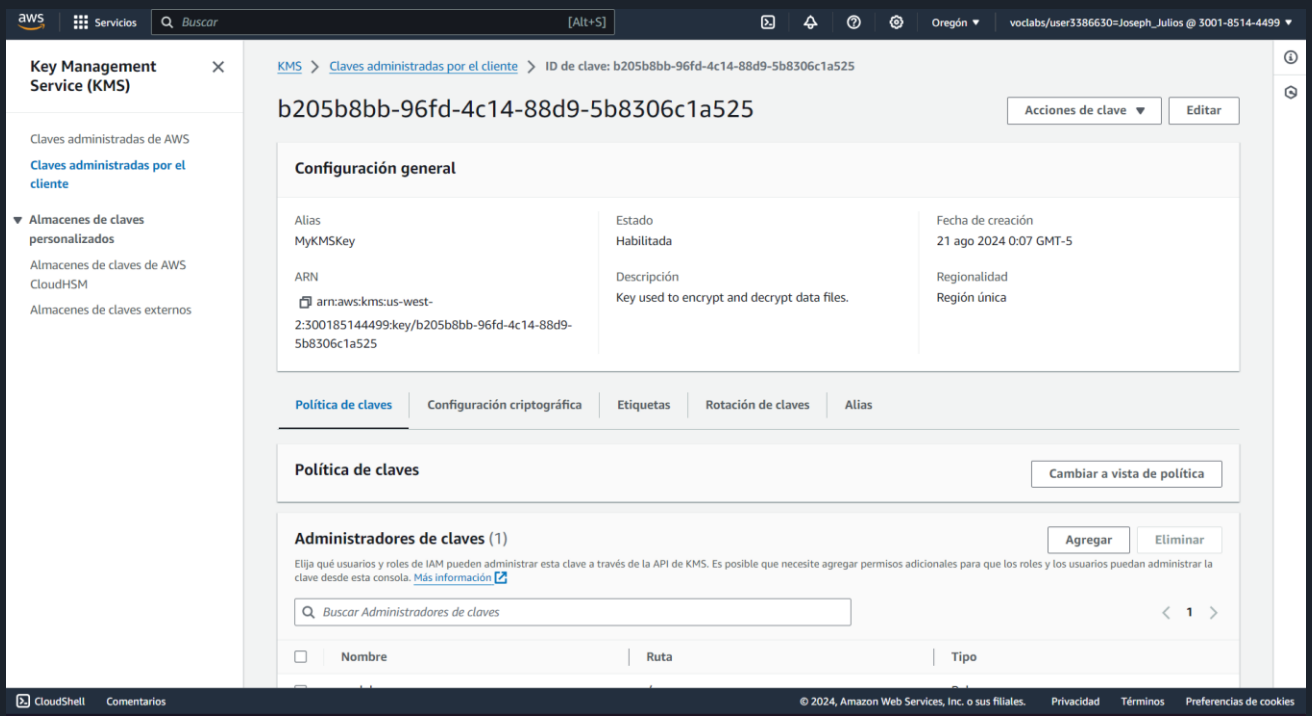
- En la página Define key administrative permissions, en la sección Key administrators, busque y seleccione la casilla para voclabs y luego seleccione Next.



- En la página Define key usage, en la página This account, busque y seleccione la casilla para voclabs y luego seleccione Next. Revise la configuración y luego seleccione Finish.



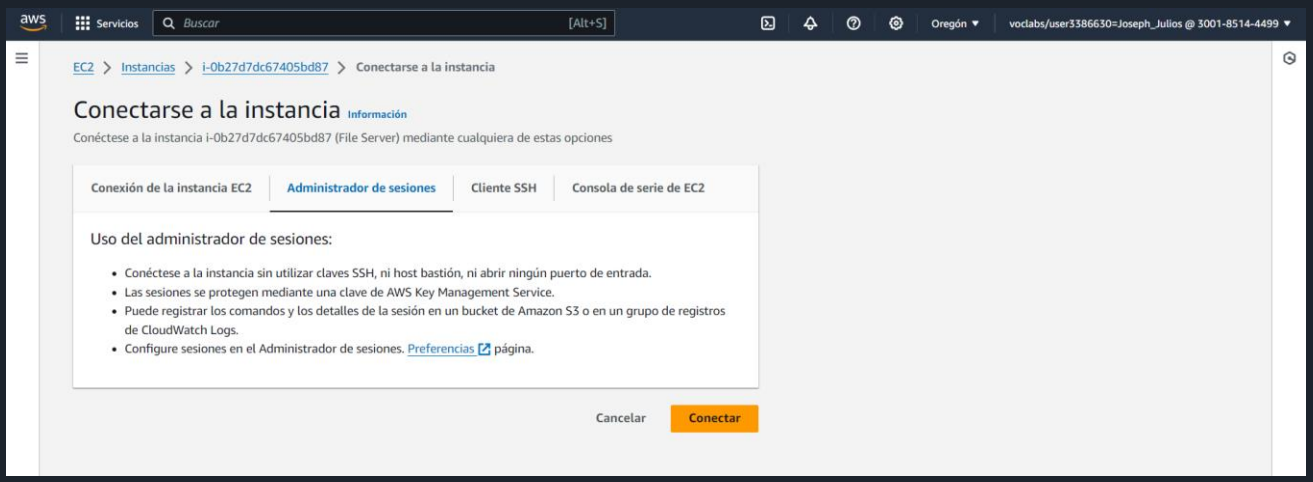
- Copie el enlace para MyKMSKey, que acaba de crear, y copie el valor ARN a un editor de texto.



TAREA 2

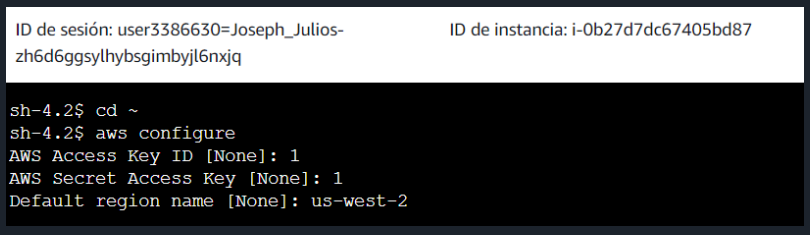
Antes de que pueda cifrar y descifrar datos, debe configurar algunas cosas. Para usar su clave AWS KMS, configurará credenciales de AWS en la instancia de EC2 de File Server (Archivo de servidor). Después, instalará la CLI de AWS Encryption (aws-encryption-cli), que puede usar para cifrar y descifrar comandos.

- En la consola, ingrese EC2 en la barra de búsqueda y luego seleccione EC2.
- En la lista Instances, seleccione la casilla a su lado para la instancia de File Server y luego seleccione Connect.
- En la pestaña Session Manager, elija Connect.

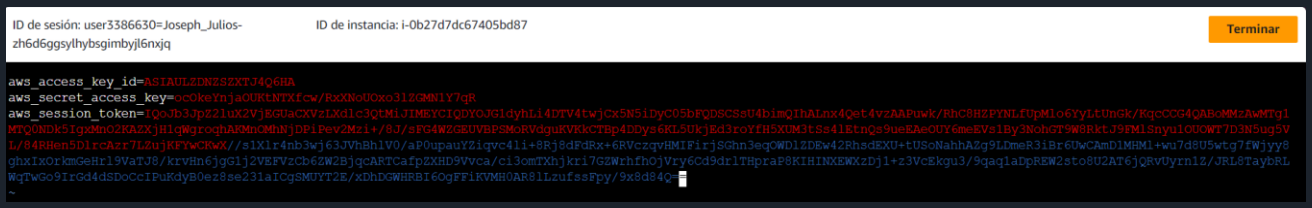


- Para cambiar el directorio principal y crear el archivo de credenciales de AWS, ejecutar aws configure.

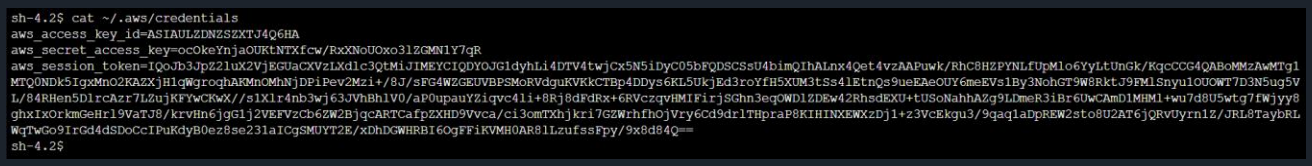
- Cuando se le solicite, configure los siguientes ajustes.



- Navegue hasta la página de la consola de Vocareum y seleccione el botón AWS Details.
- Junto a AWS CLI, seleccione Show.
- Copie y pegue el bloque de código, que comienza con [default] (predeterminado), en un editor de texto.
- Vuelva a la pestaña del navegador en la que inició sesión en el Servidor de archivos.
- Ejecutar *vi ~/.aws/credentials* Para abrir el archivo de credenciales de AWS.
- Vuelva a la pestaña del navegador en la que inició sesión en el Servidor de archivos.
- Pegue el bloque de código que copió de Vocareum.



- Para guardar y cerrar el archivo, presione Escape, escriba *:wq* y luego presione Intro.
- Ejecutar *cat ~/.aws/credentials* para ver los contenidos actualizados del archivo.



TAREA 3

En esta tarea, creará un archivo de texto con información confidencial ficticia. Luego, usará el cifrado para asegurar los contenidos del archivo. Luego, descifrará los datos y verá los contenidos del archivo.

- Crear un archivo de texto.
- Ver los contenidos del archivo secret1.txt.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ touch secret1.txt secret2.txt secret3.txt
sh-4.2$ echo 'TOP SECRET 1!!!' > secret1.txt
sh-4.2$ cat secret1.txt
TOP SECRET 1!!!
sh-4.2$
```

- Crear un directorio en el que crear el archivo cifrado.
- Ejecutar *keyArn=(KMS ARN)* en un editor de texto, reemplace *(KMS ARN)* con el AWS KMS ARN que copió en la tarea 1.
- Ejecute el comando actualizado en el terminal del Servidor de archivos.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ mkdir output
sh-4.2$ keyArn=(KMS ARN)
sh-4.2$ keyArn=arn:aws:kms:us-west-2:300185144499:key/b205b8bb-96fd-4c14-88d9-5b8306c1a525
sh-4.2$
```

- Cifrar el archivo secret1.txt.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ aws-encryption-cli --encrypt \
>                          --input secret1.txt \
>                          --wrapping-keys key=$keyArn \
>                          --metadata-output ~/metadata \
>                          --encryption-context purpose=test \
>                          --commitment-policy require-encrypt-require-decrypt \
>                          --output ~/output/.
sh-4.2$
```

- Determinar si el comando se realizó correctamente.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq ID de instancia: i-0b27d7dc67405bd87

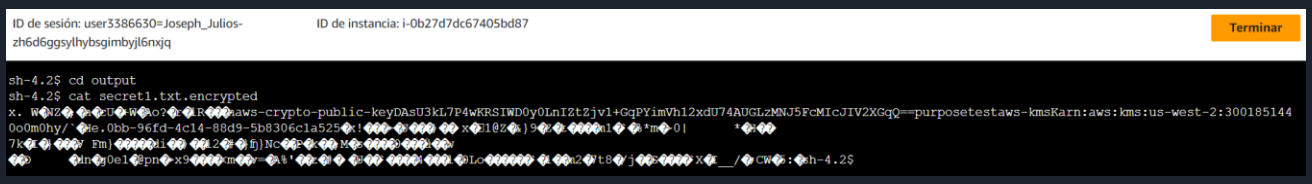
```
sh-4.2$ echo $?
0
sh-4.2$
```

- Ver la ubicación del archivo recién cifrado.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ ls output
secret1.txt.encrypted
sh-4.2$
```

- Ver los contenidos del archivo recién cifrado.



- Descifrar el archivo.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ aws-encryption-cli --decrypt \
>                       --input secret1.txt.encrypted \
>                       --wrapping-keys key=$keyArn \
>                       --commitment-policy require-encrypt-require-decrypt \
>                       --encryption-context purpose=test \
>                       --metadata-output ~/metadata \
>                       --max-encrypted-data-keys 1 \
>                       --buffer \
>                       --output .
sh-4.2$
```

- Ver la ubicación del nuevo archivo.
- Ver los contenidos del archivo descifrado.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ ls
secret1.txt.encrypted  secret1.txt.encrypted.decrypted
sh-4.2$ cat secret1.txt.encrypted.decrypted
TOP SECRET 1!!!
sh-4.2$
```